Microsoft

70-642

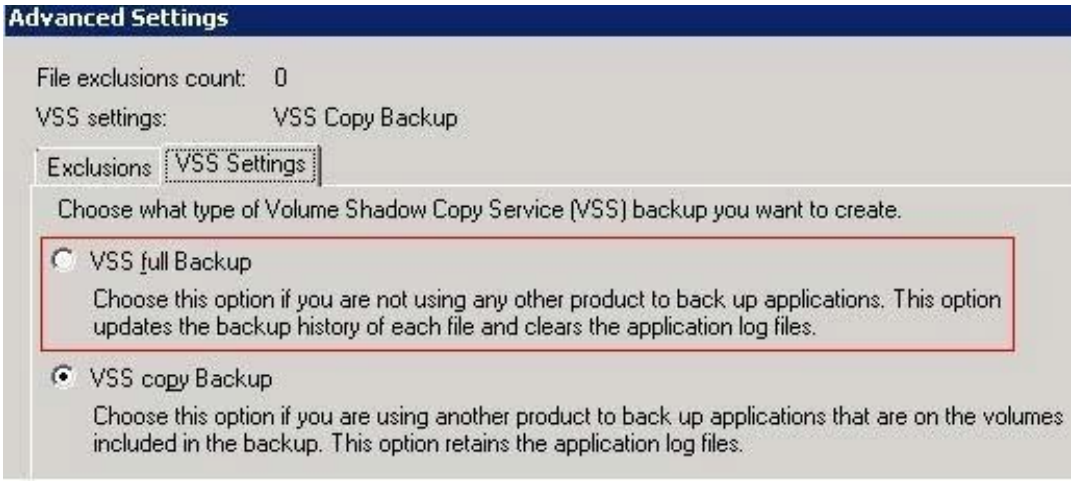
TS: Windows Server 2008 Network Infrastructure, Configuring

QUESTION: 160
Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has Microsoft Exchange Server 2010 deployed. You schedule a backup of the server. You discover that the Exchange Server 2010 transaction log files are purged during the backup. You need to prevent the Exchange Server 2010 transaction log files from being purged. What should you do?

A. From the properties of the backup, add an exclusion.
B. From the properties of the backup, modify the VSS settings.
C. From Windows PowerShell, run the New-WBFileSpec cmdlet.
D. From Windows PowerShell, run the New-WBBackupTarget cmdlet.

Answer: B

Explanation:



QUESTION: 161
Your network contains a file server that runs Windows Server 2008 R2. The server has File Server Resource Manager (FSRM) installed. A file screen is created for a folder named Data. Data is located on the C drive. The file screen is configured to block files contained in the Audio and Video file group. You need to allow users in the sales department to upload video files to C:\Data\Sales. What should you do?

A. Crate a file screen exception.
B. Modify the Audio and Video file group.
C. Implement an active file screen on C:\Data\Sales.
D. Implement a passive file screen on C:\Data\Sales.

Answer: A

Explanation:
With File screen exceptions, expand the flexibility of the file screening capabilities in File Server Resource Manager by creating an exception to any file screening rules derived from a parent folder (C:\Data).

QUESTION: 162
Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the File
Services role installed.
You configure a file classification rule.
You discover that scanned documents stored as JPG files are not being classified. You need to ensure that all file classification rules apply to scanned documents. What should you do?

A. Enable the Windows TIFF IFilter feature.
B. Modify the properties of the file classification rule.
C. Modify the properties of the Windows Search Service.
D. Install the Office 2007 System Converter: Microsoft Filter Pack.

Answer: A

Explanation:
1- Not classified as a matter of operation to the file. As soon the file "steps onto the ground" - I mean being copied to NTFS File system if there is a classification rule/pattern that match file strings it will apply;
2 - If there is a classification rule for a "JPG" file format at all - it will classify the scanned JPGs,
3 - This might be our winner!! =)) The word "document" A) Enable the Windows TIFF IFilter feature. Cheers! =)
In order FCI /File Classification Infrastructure/ to classify images based on their content by using optical character recognition (OCR), you need to install Windows TIFF IFilter on the server that is running FCI. Then the content classifier can recognize TIFF images and extract text from those files TIFF IFilter supports the most frequent compressions, such as LZW, JPG, CCITT v4, CCITT v6, uncompressed, and so forth.
"You discover that scanned documents stored as JPG files are not being classified. You need to ensure that all file classification rules apply to scanned documents." So, we have "Folder"and
"Content" classifiers types. =Folder Classifier:
- This rule uses the Folder Classifier which assigns the specified value to the classification property for all files within the rule's scope /within the target folder/.

Which means that this mechanism does not "care" for a file type or whatever is the operation that created the file in the set for classification folder... as soon the file is in the folder - it will be classified. ;)
=Content Clasifier:
- Searches for text or patterns using the same mechanism as the search indexer and if it finds them assigns the specified value to the classification property. When parameters are found in a file, then the rule will assign the property value /Example : If a word/string "Confidential" is set in the rule and there is a file containing that word
- file will be classified./
So we have tree "magic words" mentioned as a factors for the not-classified files in the "Question"
1. File is scanned to the server
2. File type is JPG
3. File subject - contains document

QUESTION: 163
Your network contains a file server named Server1 that runs Windows Server 2008 R2. On Server1, you create a disk quota for volume E that limits storage to 200 MB for all users. You need to ensure that a user named User1 can store files that are larger than 200 MB on volume E.
What should you do?

A. From File Server Resource Manager, create a file screen exception.
B. From a command prompt, run dirquota.exe.
C. From Disk Management, create a new quota entry.
D. From Windows Explorer, modify the security properties of the volume.

Answer: C

Explanation:
You can set quota limits on individual users, or you can have limits apply equally to all non- administrative users. Unfortunately, you can't set limits on groups of users. And any users who already own files on the disk will have their quotas initially disabled. New users will have the default quotas for the disk applied as you would expect when they first save a file on the disk. To set the quotas for individual users, follow these steps: In Disk Management, right-click a drive letter and open the properties of that drive. Click the Quota tab, and then click Show Quota Settings to bring up the Quota Settings dialog box for that disk.
Click Quota Entries to open the Quota Entries dialog box for the disk.
- To create a quota for a user who doesn't have one yet, and who needs a quota different from the default for the disk, click New Quota Entry.

- To modify the quota for a user already listed, select the user and then click Properties to open the quota settings for that user. Set the quota for the user and click OK to return to the Quota Entries dialog box.

QUESTION: 164
Your networ contains a file server named Server1 that runs Windows Server 2008 R2. Server1 has a volume named E.
From the File Server Resource Manager console, you create a new quota for volume E. The quota is derived from the 100 MB limit quota template.
You need to prevent users from storing audio and video files on volume E. What should you do?

A. Create a file screen.
B. Create a file management task.
C. Modify the properties of the quota.
D. Modify the properties of the Audio and Video Files file group.

Answer: A

Explanation:
Create a File Screen to prevent users from saving of video/audio files to a share and send notifications when users attempt to do that.

QUESTION: 165
Your network contains a file server named Server1 that runs Windows Server 2008 R2. You have a folder named Folder1.
You need to ensure that files in Folder1 that are older than 365 days are automatically moved to an archive folder.
What should you create from the File Server Resource Manager console?

A. a file group
B. a file management task
C. a file screen
D. a quota

Answer: B

Explanation:
You can use file management tasks to perform the following actions:
- Create and update file expiration tasks, which move all files that match a set of criteria to a specified directory where an administrator can then back up and delete

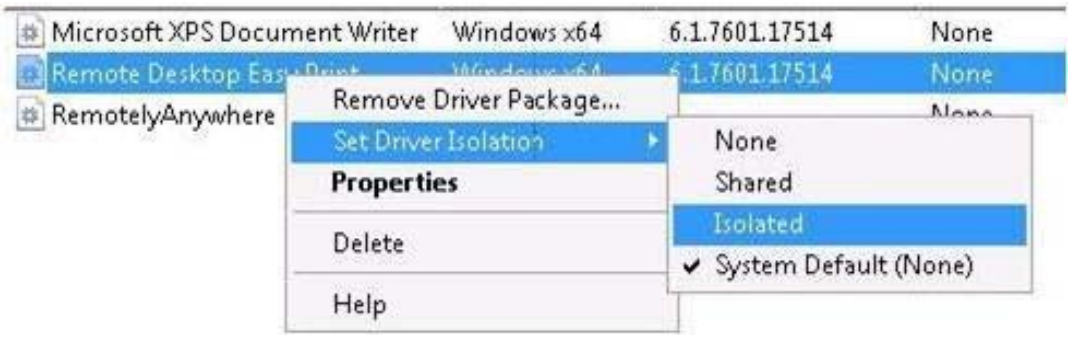
the files. Files can be set to expire based on classification values, or after a specified number of days since the file was created, modified, or last accessed.
- Create and update custom tasks, which allow you to run a command or script in a specified working directory.
- Send e-mail notifications, send a warning to the event log, or run a command or script at a specified number of days before the file management task is scheduled to run.

QUESTION: 166
Your network contains a print server named Server1. Server1 has three shared printers named Printer1, Printer2, and Printer3. Each shared printer uses a different driver. You need to ensure that if Printer1 causes an exception, users can still print to Printer2 and
Printer3.
What should you do?

A. Add a driver filter.
B. Add a printer filter.
C. Modify the print processor options.
D. Modify the driver isolation settings.

Answer: D

Explanation:



QUESTION: 167
Your network contains an Active Directory domain. You have a print server named Server1 that runs Windows Server 2008 R2. You deploy a new print device and create a shared printer. You need to ensure that only members of a group named Marketing can print color documents on the new print device. All other users must only be able to print black and white documents on the new print device. What should you do?

A. Create a printer port.
B. Create a second shared printer.
C. Modify the Active Directory printer object.
D. Modify the properties of the shared printer.

Answer: B

QUESTION: 168
Your network contains an Active Directory domain. The domain contains a print server named
Server1.
Server1 runs Windows Server 2008 R2.
You need to ensure that users can locate all shared printers on Server1 by using Active Directory.
What should you do from Server1?

A. Run the pubprn.vbs script.
B. Run dism.exe.
C. Run the Set-ADObject cmdlet.
D. Modify the Print Server properties.

Answer: A

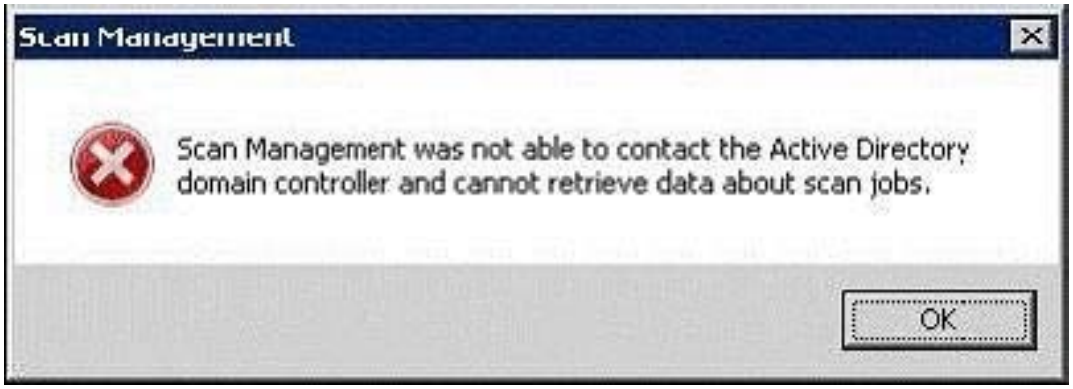
Explanation:
The script pubprn.vbs publishes a printer to the Active Directory Domain Services.

QUESTION: 169
Your network contains an Active Directory domain. The domain contains two print servers named
Server1 and Server2 that run Windows Server 2008 R2.
Server1 has a printer named Printer1. Server2 has a printer named Printer2. Both printers use the same driver.
The print device for Printer1 fails.
You need to ensure that the print jobs in the Printer1 queue are printed. What should you do?

A. Modify the Ports settings of Printer1.
B. Modify the Sharing settings of Printer1.
C. Run the Printer Migration tool.
D. Run the Remove-Job and Copy-Item cmdlets.

Answer: A

QUESTION: 170
Your network contains an Active Directory domain named contoso.com. The functional level of the domain and the functional level of the forest are Windows Server 2003. All domain controllers run Windows Server 2008.
You have a member server that runs Windows Server 2008 R2 named Server1. You install the Distributed Scan Server role service on Server1. From the Scan Management console, you attempt to add a scan process and you receive the following error.



You need to ensure that you can add a scan process.
What should you do?

A. Install the Fax Server role.
B. Install the Print Server role service.
C. Update the Active Directory schema.
D. Set the functional level of the forest to Windows Server 2008.

Answer: C

Explanation:
In order to use DSM its needed to upgrade the AD Schema thats found here - http://www.microsoft.com/en-us/download/details.aspx?id=9494
http://blogs.technet.com/b/askperf/archive/2009/10/11/windows-7-windows-server-2008-r2- distributedscanmanagement.aspx
http://blogs.technet.com/b/print/archive/2009/10/22/distributed-scan-management.aspx

QUESTION: 171
Your network contains a Windows Server Update Services (WSUS) server. All computers on the network are configured to download and install updates once a week. You need to deploy a critical update to a WSUS client as soon as possible. Which command should you run?

A. dism.exe /online /check-apppatch
B. gpupdate.exe /force
C. secedit.exe /refreshpolicy
D. wuauclt.exe /detectnow

Answer: D

Explanation:
Manipulate Automatic Updates Behavior Using Command-line Options There are two documented commandline options used for manipulating Automatic Updates behavior. These options are meant to be run from a command prompt. They are helpful for testing and troubleshooting client computers. For comprehensive troubleshooting information for problems with both the WSUS server and client computers, see "Microsoft Windows Server Update Services Operations Guide."
Detectnow Option Because waiting for detection to start can be a time-consuming process, an option has been added to allow you to initiate detection right away. On one of the computers with the new Automatic Update client installed, run the following command at the command prompt: wuauclt.exe /detectnow

QUESTION: 172
Your network contains a Windows Server Update Services (WSUS) server named Server1. Server1 provides updates to client computers in two sites named Site1 and Site2. A WSUS computer group named Group1 is configured for automatic approval. You need to ensure that new client computers in Site2 are automatically added to Group1. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Create a new automatic approval update rule.
B. Modify the Computers Options in the Update Services console.
C. Modify the Automatic Approvals options in the Update Services console.
D. Configure a Group Policy object (GPO) that enables client-side targeting.

Answer: B, D

Explanation:
http://technet.microsoft.com/en-us/library/cc720433(WS.10).aspx

WSUS enables you to target updates to groups of client computers. This capability can help you ensure that specific computers get the right updates at the most convenient times on an ongoing basis. For example, if all computers in one department of your organization have a specific configuration (such as all computers in the Accounting team), you can determine what updates those computers get, at what time, and then use WSUS reporting features to evaluate the success of update activity for that computer group.

By default, each computer is already assigned to the All Computers group. Computers will also be assigned to the Unassigned Computers group until you assign them to another group.

Regardless of the group you assign a computer to, it will also remain in the All Computers group. A computer can be in only one other group in addition to the All Computers group.

You can assign computers to computer groups by using one of two methods, server-side targeting or client side targeting, depending on whether or not you want to automate the process. With server-side targeting, you use the Move the selected computer task on the Computers page to move one or more client computers to one computer group at a time. With client-side targeting, you use Group Policy or edit the registry settings on client computers to enable those computers to automatically add themselves into the computer groups. You must specify which method you will use by selecting one of the two options on the Computers Options page.

Note

If your WSUS server is running in replica mode, you will not be able to create computer groups on that server, you will only inherit the computer groups created on the administration server from which your server inherits its settings. For more information about replica mode, see Running in Replica Mode.

Server-side Targeting With server-side targeting, you use the WSUS console to both create

groups and then assign computers to the groups. Server-side targeting is an excellent option if you do not have many client computers to update and you want to move client computers into computer groups manually.

To enable server-side targeting on your WSUS server, click the Use the Move computers task in

Windows Server Update Services option on the Computers Options page.

Client-side Targeting With client-side targeting, you enable client-computers to add themselves to the computer groups you create in the WSUS console. You can enable client-side targeting through Group Policy (in an Active Directory network environment) or by editing registry entries (in a non-Active Directory network environment) for the client computers. When the client computers connect to the WSUS server, they will add themselves into the correct computer group. Client-side targeting is an excellent option if you have many client computers and want to automate the process of assigning them to computer groups. To enable client-side targeting on your WSUS server, click the Use Group Policy or registry settings on client computers option on the

Computers Options page.

QUESTION: 173
Your network contains an Active Directory domain. The domain contains a Windows Server Update Services (WSUS) server named Server1. A Group Policy object (GPO) named GPO1 configures all computers in the domain to use Server1 for Windows Update. You add a new Windows 7 computer named Computer1 to the domain.
From the Update Services console, you discover that Computer1 is not listed as a member of any computer groups.
You verify that GPO1 is applied to Computer1.
You need to ensure that Computer1 is available in the Update Services console. What should you do?

A. On Computer1, run wuauclt.exe /detectnow.
B. On Computer1, run wuauclt.exe /reportnow.
C. On Server1, run wsusutil.exe reset.
D. On Server1, run wsusutil.exe listinactiveapprovals.

Answer: A

Explanation:
Automatic Updates Behavior Using Command-line Options There are two documented command- line options used for manipulating Automatic Updates behavior. These options are meant to be run from a command prompt. They are helpful for testing and troubleshooting client computers. For comprehensive troubleshooting information for problems with both the WSUS server and client computers, see "Microsoft Windows Server Update Services Operations Guide."
Detectnow Option Because waiting for detection to start can be a time-consuming process, an option has been added to allow you to initiate detection right away. On one of the computers with the new Automatic Update client installed, run the following command at the command prompt: wuauclt.exe /detectnow
Resetauthorization Option
WSUS uses a cookie on client computers to store various types of information, including computer group membership when client-side targeting is used. By default this cookie expires an hour after WSUS creates it. If you are using client-side targeting and change group membership, use this option in combination with detectnow to expire the cookie, initiate detection, and have WSUS update computer group membership.
Note that when combining parameters, you can use them only in the order specified as follows:
wuauclt.exe /resetauthorization /detectnow http://technet.microsoft.com/en-us/library/cc708617(v=WS.10).aspx

QUESTION: 174

Your network contains a Windows Server Update Services (WSUS) server. A Group Policy object (GPO) configures all WSUS client computers to detect updates hourly and install updates weekly. You download a critical update.
You need to ensure that the WSUS client computers install the critical update during the next detection interval. What should you do?

A. From the client computers, run wuauclt.exe /force.
B. From the client computers, run gpupdate.exe /force.
C. From the server, configure the deadline settings.
D. From the server, configure the Synchronization Schedule options.

Answer: C

Explanation:
In your server, you can specify a deadline when you approve an update or set of updates on the
WSUS server.
Setting a deadline will cause clients to install the update at a specific time, but there are a number
of different situations, depending on whether the deadline has expired, whether there are other updates in the queue for the client to install, and whether the update (or another update in the queue) requires a restart.
http://technet.microsoft.com/en-us/library/cc708585(v=ws.10).aspx